



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/391,360	09/07/1999	PAUL R. CARPENTIER	WRSHPO04	8493

24227 7590 05/21/2004
EMC CORPORATION
OFFICE OF THE GENERAL COUNSEL
176 SOUTH STREET
HOPKINTON, MA 01748

EXAMINER

HA, LEYNNA A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 05/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application N .

09/391,360

Applicant(s)

CARPENTIER ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-30 has been re-examined and newly added claims have been examined. This is a FINAL rejection due to new grounds of rejection.
2. Claims 1-5, 7-10, 13, 14, 18, and 20-30 remains rejected under 35 U.S.C. 102(e).
3. Claims 6, 11, 12, 15-17, and 19 remains rejected under 35 U.S.C. 103(a).
4. Claims 31-33 are rejected remains rejected under 35 U.S.C. 102(e).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore,

the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1-5, 7-10, 13,14, 18, and 20-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Saito (US 6,076,077).

As per claim 1:

Saito discloses a method of producing an encrypted version of a binary asset wherein for purposes of applying art, can be in the form of a file or data content (col.7, line 10-28). The method comprising a unique identifier (UID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.7, lines 38-55). It is inherent a key is an identifier for a record in a datafile and because a key is inherently unique the referenced data of the file can be retrieved by the key that belongs to that particular datafile. The file is encrypted with a key, which results an encrypted file (col.7, line 60-col.8, lines 67).

As per claim 2:

Saito discloses a second UID for the encrypted version of the file (col.11, lines 32-42) that is computed from at least a portion of the encrypted version (col.19, lines 38-45) wherein the second UID is use for retrieval of the encrypted file (col.19, lines 60-63). In order to retrieve or obtain the encrypted file, it is necessary to use the private key of the second UID (encrypted original secret key) to decrypt the encrypted file.

As per claim 3:

Saito discloses a first identifier that identifies the descriptor file and encrypting the file using the first file identifier as a key (col.22, lines 29-32). Further, Saito generating a second identifier that identifies the encrypted descriptor file (col.22, lines 33-50) wherein the first and second identifiers are used to access the contents of the binary asset (col.22, line 54 thru col.23, line 3).

As per claim 4:

Saito discloses a method of producing an encrypted version of a file or data content (col.7, line 10-67). The method comprising a file identifier (F-ID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.12, lines 40-63). It is inherent a key is an identifier for a record in a datafile and because a key is inherently unique the referenced data of the file can be retrieved by the key that belongs to that particular datafile. The file is encrypted with a key, which results in encrypted file (col.7, line 60-col.8, lines 67). Further, Saito teaches providing the key to decrypt the encrypted file to verify the integrity of the decrypted file (col.9, lines 19-40). Saito discloses a second F-ID for the encrypted version of the file wherein is used to retrieve (by decrypting) the encrypted file (col.9, lines 19-24 and col.8, lines 56-67).

As per claim 5:

Saito uses a hash function (col.12, lines 55-57 and col.14, lines 36-43).

Art Unit: 2135

As per claim 7: As rejected with the same rationale in claim 2.

As per claim 8:

Saito discloses a method of producing an encrypted version of a binary asset wherein for purposes of applying art, can be in the form of a file or data content (col.7, line 10-28). The method comprising a unique identifier (UID) that was generated for the file that was computed from at least a portion of the contents uniquely identifies the file as intrinsic (col.7, lines 38-55). It is inherent a key is an identifier for a record in a datafile and because a key is inherently unique the referenced data of the file can be retrieved by the key that belongs to that particular datafile. The file is encrypted with a key, which results in encrypted file (col.7, line 60-col.8, line 18). Further, Saito teaches providing the key to decrypt the encrypted file to verify the integrity of the decrypted file (col.9, lines 19-40). Also refer to col.8, lines 20-59 and col.10, line 5, ET. Seq.

As per claim 9: Saito includes the method comprising a unique identifier (UID) that was generated for the file that was computed from at least a portion of the contents where the Examiner asserts that uniquely identifies the file as intrinsic (col.7, lines 38-55)..

As per claim 10: As rejected with the same rationale as rejected in claim 5.

As per claim 12: As rejected with the same rationale as rejected in claim 5.

As per claim 13:

Saito discloses a structure for reliably identifying plurality of files comprising a file name for the files and Meta data for each file indicating attributes for each file (col.10, lines 57-65). It is inherent that Meta data is data about data, which constitute attributes such as the title, subject, author, file size, and etc. of the file. In addition, Saito discloses a unique identifier (UID) that was generated for the file that was computed from at least a portion of the contents where uniquely identifies the file as intrinsic (col.7, lines 38-55). It is inherent a key is an identifier for a record in a datafile and because a key is inherently unique the referenced data of the file can be retrieved by the key that belongs to that particular datafile. The file is encrypted with a key, which results in encrypted file (col.7, line 55). Further, Saito teaches providing the key to decrypt the encrypted file to verify the integrity of the decrypted file (col.8, lines 1-10). Also refer to col.8, lines 20-59 and col.10, line 5, ET. Seq.

As per claim 14: As rejected with the same rationale as rejected in claim 13.

As per claim 18: As rejected with the same rationale as rejected in claim 13.

Also, see col.14, lines 56-67.

As per claim 20: As rejected with the same rationale as rejected in claim 16.

As per claim 21:

Saito discloses a master identifier that identifies the encrypted file and retrieving the encrypted file using the first master identifier (col.22, lines 28-34). Saito discusses receiving the key identifier of the non-encrypted version of

the encrypted file and decrypting the encrypted file using the key identifier to obtain the non-encrypted version (col.22, lines 45-62), which includes data file identifier that identifies the data, and the encrypted version of the data file (col.23, lines 10-13). Further, Saito discusses retrieving the encrypted version of the data file using the encrypted identifier and decrypting the encrypted data file using the data file identifier as a decryption key whereby, the non-encrypted version of the data file is obtained (col.22, line 65 thru col.23, line 3).

As per claim 22:

Saito discloses a structure for reliably identifying plurality of files comprising file names and Meta data for each file (col.10, lines 57-65).

As per claim 23: Saito discloses a method of producing an encrypted version of a file (col.7, line 10-28). Saito teaches encrypting and decrypting wherein the method comprises a file identifier (F-ID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.7, lines 38-55) and encrypts and decrypts the file with the F-ID as the key (col.9, lines 18-22).

As per claim 24:

Saito includes the digital signature and the key is used to authenticate the non-encrypted file (col.14, lines 1, Et Seq.).

As per claim 25: As rejected with the same rationale as rejected in claim 24.

As p r claim 26:

Saito discloses a method of producing an encrypted version of a file (col.7, line 10-28). Saito teaches encrypting and decrypting wherein the method comprises a file identifier (F-ID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.7, lines 38-55) and encrypts and decrypts the file with the F-ID as the key.

Saito discloses a descriptor file that includes the first identifier and the second identifier (col.8, lines 45-58) wherein the first identifier and the second identifier are used for encryption (col.12, lines 40-64).

Further, Saito discloses structure for reliably identifying plurality of files comprising a file name for the files and Meta data for each file indicating attributes for each file (col.10, lines 57-65). It is inherent that Meta data is data about data, which constitute attributes such as the title, subject, author, file size, and etc. of the file. Also, refer to col.13, ET Seq.

As per claim 27: As rejected with the same rationale as rejected in claim 22.

As per claim 28: As rejected with the same rationale as rejected in claim 23.

As per claim 29: As rejected with the same rationale as rejected in claim 24.

As per claim 30: As rejected with the same rationale as rejected in claim 25.

As per claim 31:

Saito discusses decrypting the encrypted version using the F-ID to generate a decrypted version of the binary asset (col.9, lines 14-40).

Also refer to col.10, line 5, ET. Seq.

As per claim 32: See col.14, lines 35-43; discusses verifying the integrity of the decrypted version.

As per claim 33: See col.14, lines 35-43; discusses first and second same hash functions being compared to in order to verify the validity.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 6, 11, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito as applied to claims 4, 8, and 18 above, and further in view of Berkowitz, et al. (US 5,832,479).

As per claim 6:

Saito discloses a method of producing an encrypted version of a file or data content (col.7, line 10-28). The method comprising a file identifier (F-ID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.7, lines 38-55). However, Saito fails to include compressing a file.

Berkowitz, et al. discloses a method for storing data wherein each document has a unique document identifier and data keys (col.1, lines 52-65). Berkowitz includes a step of providing data key identifier and further compressing the file (col.4, lines 28-52). The Examiner asserts compressing the file helps reduce the size of the data therein so that less space is needed and less bandwidth is needed to transmit the file. Therefore, it would have been obvious to modify the encrypting of the file of Saito, in conjunction with the step of compressing the file of, Berkowitz, because the data size is reduced or minimized to express transmission of the file (col.4, lines 59-65).

As per claim 11: As rejected with the same rationale as rejected in claim 6.

As per claim 19:

Saito discloses a method of producing an encrypted version of a file (col.7, line 10-28). Saito teaches encrypting and decrypting wherein the method comprises a file identifier (F-ID) that was generated for the file that was computed from at least a portion of the contents and that uniquely identifies the file (col.7, lines 38-55) and encrypts and decrypts the file with the F-ID as the key. However, Saito fails to include decompressing a file in conjunction with decrypting.

Berkowitz, et al. discloses a method for storing data wherein each document has a unique document identifier and data keys (col.1, lines 52-65). Berkowitz includes a step of providing data key identifier and further compressing the file but fails to explicitly include the step of decompressing the

encrypted version of the file in conjunction with decrypting (col.4, lines 28-52). The Examiner asserts that Berkowitz teaches compressing the file in order to reduce the size and the bandwidth when transmitting but cannot view in its compressed state. Thus, it is inherent to decompress when decrypting the file in order to restore the contents to its original form. It would have been obvious for a person of ordinary skill in the art to decompress the file because it restores the contents of the compressed file to its original form in order to view the file (col.4, lines 59-65).

8. Claims 12 and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito, and further in view of "Microsoft Computer Dictionary, 5th Edition".

As per claim 12:

Saito discloses a method of producing an encrypted version of a file or (col.7, line 10-28) wherein a unique identifier (UID) is generated for the file that was computed from at least a portion of the contents where the Examiner asserts that uniquely identifies the file as intrinsic (col.7, lines 38-55). In addition, Saito teaches the ability to create different format of files such as digital content in encrypted form (col.6, lines 30-65 and col.8, lines 34-40), however, Saito fails to include a flattened file.

According to the "Microsoft Computer Dictionary, 5th Edition", to "flatten" is to combine all layers of text or images into a single layer (pg.217). It would

have been obvious for a person of ordinary skill in the art to combine the teaching of, "Microsoft Computer Dictionary, 5th Edition", by creating a flattened file for the different format of files as taught by, Saito, because it significantly reduces its file sized and can be saved in a wider range of formats.

As per claim 15:

Saito discloses a method of producing an encrypted version of a file or (col.7, line 10-28) wherein a unique identifier (UID) is generated for the file that was computed from at least a portion of the contents where the Examiner asserts that uniquely identifies the file as intrinsic (col.7, lines 38-55). Saito includes a key control center for storing crypt keys that are used for decryption (col.10, lines 30-39). It is inherent a key is an identifier for a record in a datafile and because a key is inherently unique the referenced data of the file can be retrieved by the key that belongs to that particular datafile. The file is encrypted with a key, which results in encrypted file (col.7, line 60-col.8, line 18). The file is encrypted with a key, which results in encrypted file (col.7, line 60-col.8, line 18). Further, Saito teaches providing the key to decrypt the encrypted file to verify the integrity of the decrypted file (col.9, lines 19-40).

In addition, Saito teaches the ability to create different format of files such as digital content in encrypted form (col.6, lines 30-65 and col.8, lines 34-40), however, Saito fails to include a flattened file.

According to the "Microsoft Computer Dictionary, 5th Edition", to "flatten" is to combine all layers of text or images into a single layer (pg.217). It would

Art Unit: 2135

have been obvious for a person of ordinary skill in the art to combine the teaching of, "Microsoft Computer Dictionary, 5th Edition", by creating a flattened file for the different format of files as taught by, Saito, because it significantly reduces its file sized and can be saved in a wider range of formats.

As per claim 16: As rejected with the same rationale as rejected in claim 15.

As per claim 17:

Saito discloses a method a structure for reliably identifying plurality of files comprising file names and Meta data for each file (col.10, lines 57-65).

Response to Amendment

9. Applicant's arguments with respect to claims 1-33 have been considered but are moot.

It is inherent a key identifies (an identifier) for a record in a datafile and because a key is inherently unique, the referenced data of the file can be retrieved by the key that belongs to that particular datafile. Please refer to "Microsoft Computer Dictionary, 5th Edition" for the term "key" on page 300. Further, it is obvious that the key is computed from the content of the data, else how else can the key be identified belonging to that particular file if the content is of another file.

C nclusi n

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100